**En una vuelta del algoritmo criptográfico DES se tiene como entrada a las cajas S el texto hexadecimal FABADAFABADA.**

**Se pide:**

**a. Encontrar la salida de las cajas y mostrar toda la cadena de bits resultantes de la operación de las cajas S en esa vuelta en octetos.**

**FABADAFABADA** = 111110 101011 101011 011010 111110 101011 101011 011010

S1 = 111110 = 0 = 0000

S2 = 101011 = 15 = 1111

S3 = 101011 = 9 = 1001

S4 = 011010 = 12 = 1100

S5 = 111110 = 14 = 1110

S6 = 101011 = 5 = 0101

S7 = 101011 = 4 = 0100

S8 = 011010 = 0 = 0000

**00001111 10011100 11100101 01000000** = 8bits \* 4 =

32bits de salida de S-bo

**b. ¿Cuántas operaciones habría que realizar como máximo para romper la caja S7 en esa vuelta?**

4 elevado a 1 cajas elevado a 1 vuelta

**¿Cuántas operaciones habría que realizar como máximo para romper las 8 cajas de esa vuelta?**

4 elevado a 1 cajas elevado a 1 vuelta

**¿Y cuántas operaciones habría que realizar como máximo para romper las cajas S de un bloque de cifra del DES?**

4 elevado a 8 cajas elevado a 16 vuelta

**Siendo (n) la función de Euler, con los números p = 5, q = 20 y el producto n = p·q, elige la(s) afirmación(es) correcta(s):**

20 no es número primo por lo que no se puede realizar un RSA

**a. Las claves RSA se calcularán en un cuerpo con módulo n**

Cada usuario elegirá un valor de clave pública e dentro el siguiente intervalo: 1 < e < α Φn El módulo no es el de n nunca, lo da el módulo de Euler

**b. (n) = (p – 1)·(q – 1) = (5 -1)(20 – 1) = 4 · 19 = 76**

Es correcto si fuesen ambos primos. Esa simplificación solo vale para números primos

**c. El algoritmo RSA se basa en la dificultad de factorizar números primos.**

Depende del tamaño de los números

Hay que tener en cuenta que para las claves RSA actuales, con un cuerpo de cifra de al menos 1.024 bits, ninguno de estos tres ataques son viables.

**¿Cuál de las siguientes opciones es más eficiente? Justifica tu respuesta.**

**a.**

**C= Me mod n**

**C1 = Cd mod n**

**b.**

**C= Md mod n**

**C1= Ce mod n**

La respuesta es la **A**. Ahí está aplicando un cifrado y firmado. En la A se cifra y después se firma y en la B se firma y después se cifra.

**Explica, con tus propias palabras, qué es, qué características tiene y qué aplicaciones prácticas puede tener una función hash. Además, menciona las funciones hash que conozcas.**

Un Hash es un cálculo matemático realizado que transforma cualquier bloque de datos en una serie de caracteres con longitud fija. El valor de salida no varía en longitud aun siendo diferentes la longitud del contenido a calcular.

Este sistema sirve para: comprobar la integridad de los ficheros, para securización de procesos de identificación en sistemas (user/password), firmas digitales, etc.

SHA-1, SHA-2, SHA-256, SHA-3 , SHA-512, MD5